WHAT IS CLAIMED IS:

1. A method for encrypting data, the method comprising:
generating a session key;
encrypting the data utilizing the session key;
encrypting the session key utilizing a user public key;
encrypting the session key utilizing a master public key; and
generating a data packet including the encrypted data and the encrypted session keys.

2. The method, as set forth in claim 1, further comprising:
transmitting the data packet to a destination data processing system;
decrypting the session key utilizing a user private key; and
decrypting the data utilizing the session key.

3. The method, as set forth in claim 1, further comprising:
decrypting the encrypted session key with a master private key; and
decrypting the data with the session key.

4. The method, as set forth in claim 1, further comprising encrypting the session key utilizing an asymmetric encryption routine.

5. The method, as set forth in claim 1, further comprising encrypting the data utilizing a symmetric encryption routine.

6. The method, as set forth in claim 1, further comprising encrypting the session key utilizing the user's public key.

7. The method, as set forth in claim 2, further comprising storing the user's private key on a data storage medium coupled to the destination data processing system.

8. The method, as set forth in claim 3, further comprising storing the master private key on a data storage medium coupled to the destination data processing system.

9. The method, as set forth in claim 2, further comprising retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

10. The method, as set forth in claim 3, further comprising retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

11. The method, as set forth in claim 1, further comprising utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

12. A public key data encryption system wherein each user has a private key and a certificate containing data pertaining to the user including the user's public key, the encryption system comprising:

a master public key;

a first data processing system operable to generate a session key, to encrypt data using the session key, to encrypt the session key with the user's public key, to encrypt the session key with the master public key, to generate a data packet including the encrypted session keys and the encrypted data, and to transmit the data packet.

13. The public key data encryption system, as set forth in claim 12, further comprising:

a second data processing system operable to receive the data packet, to decrypt the encrypted session key with the user's private key, and to decrypt the data with the session key.

14. The public key data encryption system, as set forth in claim 12, further comprising:

a master private key; and

a second data processing system operable to receive the data packet, to decrypt the encrypted session key with the master private key, and to decrypt the data with the session key.

15. The public key data encryption system, as set forth in claim 12, wherein an asymmetric encryption routine is utilized to encrypt the session key.

16. The public key data encryption system, as set forth in claim 12, wherein a symmetric encryption routine is utilized to encrypt the data.

17. The public key data encryption system, as set forth in claim 12, wherein the user's public key is utilized to encrypt the session key.

18. The public key data encryption system, as set forth in claim 13, wherein the user's private key is stored on a data storage medium coupled to the second data processing system.

19. The public key data encryption system, as set forth in claim 14, wherein the master private key is stored on a data storage medium coupled to the second data processing system.

20. The public key data encryption system, as set forth in claim 13, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the user's private key from a smart card.

21. The public key data encryption system, as set forth in claim 14, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the master private key from a smart card.

22. The public key data encryption system, as set forth in claim 12, further comprising:

a plurality of master private keys;

a plurality of master public keys; and

a second data processing system operable to receive the data packet, to decrypt the encrypted session key with the plurality of master private keys, and to decrypt the data with the session key.

23. An article of manufacture comprising:

a computer usable medium having computer readable program code embodied therein for encrypting and decrypting data wherein each user has a private key and a public key, the article of manufacture comprising:

a master public key;

a first data processing module operable to generate a session key, to encrypt data using the session key, to encrypt the session key with the user's public key, to encrypt the session key with the master public key, to generate a data packet including the encrypted session keys and the encrypted data, and to transmit the data packet.

24. The article of manufacture, as set forth in claim 23, further comprising:

a second data processing module operable to receive the data packet, to decrypt the encrypted session key with the user's private key, and to decrypt the data with the session key.

25. The article of manufacture, as set forth in claim 23, further comprising:

a master private key; and

a second data processing system operable to receive the data packet, to decrypt the encrypted session key with the master private key, and to decrypt the data with the session key.

26. The article of manufacture, as set forth in claim 24, wherein an asymmetric encryption routine is utilized to encrypt the session key.

27. The article of manufacture, as set forth in claim 24, wherein a symmetric encryption routine is utilized to encrypt the data.

28. The article of manufacture, as set forth in claim 24, wherein the user's public key is utilized to encrypt the session key.

29. The article of manufacture, as set forth in claim 24, further comprising:

a plurality of master private keys;

a plurality of master public keys; and

a second data processing module operable to receive the data packet, to decrypt the encrypted session key with the plurality of master private keys, and to decrypt the data with the session key.